الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة التكوين والتعليم المهنيين
Ministère de la Formation et de l'Enseignement Professionnels

Centre National de l'Enseignement Professionnel à Distance (CNEPD)

المركز الوطني للتعليم المهني عن بعد (م.و.ت.م.ب)

COURS DE MAINTENANCE ET SUIVI DU RESEAUX

SERIE N°03

OBJECTIF PÉDAGOGIQUE : À la fin de cette série, les stagiaires seront capables de maintenir et d'assurer le suivi du réseau.

PLAN DE LEÇON :

I- ASSURER LA SEANCE SOFT ET HARD

1- Les virus ;
2- Type de virus ;
3- Cycle de virus ;
4- La propagation du virus ;
5- Les motivations et les causes des virus ;

II- L'ANTIVIRUS

1 - Les types d'antivirus ;
2 - Signature virale ;
3 - Contrôleur d'intégrité des programmes ;
4 - Analyse heuristique ;
5 - Analyse spectrale ;
6- Désinfestation d'un PC ;
7- Prévention ;

III- SAUVEGARDE DES DONNÉES

1- Définition ;
2- Objectifs de la sauvegarde ;
3-Types de sauvegarde ;
4- Que sauvegarder ?
5 - Les différents supports de sauvegarde ;
6 - Les outils de sauvegarde.

I- ASSURER LA SEANCE SOFT ET HARD :

1- Les virus :

Introduction :

Aujourd'hui, les virus informatiques, du fait de la grande expansion des ordinateurs, concernent un nombre impressionnant de personnes. Un virus a ainsi un très grand nombre de cibles potentielles. De plus, avec l'expansion de l'Internet, la propagation des virus (et assimilés) est plus aisée et plus rapide. Il n'est pas rare aujourd'hui de voir un virus déferler sur la planète via le réseau des réseaux en quelques jours, voire quelques heures.

Les virus sont devenus très médiatisés, les attaques étant d'une ampleur toujours plus importante. Si le grand public commence à connaître ces termes, et à y être sensibilisés, le niveau de connaissance globale sur les virus reste faible pour le plus grand nombre.

1.1- Le Virus :

Avant toute chose, il convient naturellement de définir la notion de virus informatique. Un virus est en effet une entité informatique très particulière, répondant à des critères très précis.

Dark Angel, un créateur de virus, définissait son travail ainsi : "Art de programmation destiné à détruire les systèmes des crétins". L'anecdote est amusante, mais nous verrons que la programmation de virus est rarement artistique, et que les crétins ne sont pas les seuls touchés.

Le dictionnaire propose une définition plus conventionnelle : "(mot latin, poison) Informatique : instruction ou suite d'instructions parasites, introduites dans un programme et susceptibles d'entraîner diverses perturbations dans le fonctionnement de l'ordinateur".
Néanmoins, et cela montre bien l'ignorance populaire sur ce thème, même dans cette définition, la particularité majeure du

virus n'apparaît pas. Nous pouvons en fait définir un virus de la façon suivante : "Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire."

La reproduction est en effet la notion la plus importante lorsque l'on parle de virus. Un virus s'introduit dans des fichiers qu'il souhaite infecter. Au même titre que les virus organiques, le virus informatique possède donc la caractéristique principale de se dupliquer. Les virus ont à ce titre une « vie autonome », et peuvent ainsi se propager sur le plus de machines possibles (ce qui est bien sûr l'ambition du développeur). Aujourd'hui, il existe de nombreux supports de propagation, que nous détaillerons par la suite.

De même que le virus biologique, le virus informatique a pour but d'abîmer (ou du moins d'affaiblir) le système sur lequel il est hébergé. Nous verrons ultérieurement à quel point les dégâts, que peuvent causer ces petits programmes, peuvent être lourds de conséquence.

1.2 - Le ver :

Un ver est un programme indépendant, qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et donc l'infecter. Il va simplement se copier via un réseau ou Internet, d'ordinateur en ordinateur. Ce type de réplication peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise. Comme un virus, un ver peut contenir une action nuisible du type destruction de données ou envoi d'informations confidentielles.

1.3 - Le Cheval de Troie :

Un cheval de Troie ou troyen (Trojan Horse ou Trojan) n'est ni un virus ni un ver, parce qu'il ne se reproduit pas. Un cheval de Troie introduit sur une machine a pour but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement il est utilisé pour créer une porte dérobée sur

l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet. Les opérations suivantes peuvent être effectuées par l'intermédiaire d'un cheval de Troie **:**

- Récupération des mots de passe grâce à un keylogger ;
- Administration illégale à distance d'un ordinateur ;
- Relais utilisé par les pirates pour effectuer des attaques ;
- Serveur de spam (envoi en masse des e-mails).

2- Les types de Virus :

Il existe différents types de virus, les distinctions entre eux étant plus ou moins ténues. Avant d'en dresser la liste la plus exhaustive possible, signalons que les experts en virus ne sont pas tous d'accord quant à cette classification. Nous donnons donc ici une certaine topographie, qui peut différer peu ou prou d'autres topographies.

2.1 - Virus du secteur d'amorçage :

Ces virus s'attaquent au « Boot Sector » d'un disque, c'est-à-dire son premier secteur, celui qui lui sert à démarrer. Dans le cas du disque dur principal de l'ordinateur, il s'agit du premier secteur lu au démarrage de la machine. Un tel virus est ainsi chargé à chaque démarrage, et acquiert alors un contrôle complet de la machine. Ces virus sont parmi les plus difficiles à déceler. Ils sont en effet chargés en mémoire bien avant que l'utilisateur ou un logiciel (y compris un antivirus) ne prenne le contrôle de l'ordinateur.

Ces virus remplacent le secteur d'amorce du disque infecté par une copie d'eux-mêmes, puis déplacent le secteur original vers une autre portion du disque.

2.2 - Virus d'applications :

Les virus d'applications infectent les fichiers exécutables, (notamment ceux portant les extensions .exe, .com ou .sys). Il s'agit d'un morceau de programme, souvent écrit en Assembleur, qui s'intègre au début d'un programme normal.

Pour infecter, il cherche un programme cible, et remplace le premier segment de cet exécutable par son code viral. La section originale est ajoutée en fin de programme. Au moment de l'exécution du fichier, le code viral est donc lancé en premier. Il cherche encore d'autres programmes à infecter et les infecte, par le même mécanisme. Il restaure ensuite la première section du programme infecté (qu'il avait conservée, rappelons-le), et exécute le programme de manière normale. Sa propagation est donc complètement invisible, ce qui rend ces virus très contagieux. Outre cette propagation, ce virus rentre en activité après un certain laps de temps, et corrompt des fonctions du système ou des fichiers. La gravité des attaques dépend du virus, et peut varier du simple message anodin affiché sur l'écran, à la destruction pure et simple de toutes les données de l'ordinateur.

Notons que ce genre de virus possède deux modes opératoires, dits résidents et non-résidents. Nous venons de décrire le non-résident, qui se réplique lors de l'exécution d'un fichier infecté. A l'inverse, le résident s'installe dans la mémoire vive dès sa première exécution, et reste ainsi actif jusqu'à l'extinction de l'ordinateur. Dès qu'un programme non infecté est exécuté, le virus l'infecte. L'utilisateur fournit ainsi lui-même les cibles au virus, qui s'attaque à tous les programmes lancés. Certains d'entre eux résistent au simple redémarrage de l'ordinateur.

La détection de ce genre de virus est cependant assez aisée, ne serait-ce qu'en contrôlant la taille des exécutable. Le fichier infecté est en effet plus grand que son homologue sain, puisqu'il contient le code du virus en plus du programme.

2.3 - Virus furtifs :

Les virus furtifs sont très difficiles à détecter, en ce qu'ils renvoient une image du système ressemblant à ce qu'il était avant l'infection. On les appelle également des intercepteurs d'interruption. Il s'agit de tromper l'antivirus sur l'état des fichiers infectés. Ils modifient le fonctionnement du système d'exploitation, de telle sorte que les fichiers infectés semblent sains.

Une autre technique de furtivité des virus est de faire croire au système d'exploitation que des secteurs du disque dur sont défectueux. Il suffit alors au virus de s'y camoufler et d'y couler des jours paisibles en attendant son activation. Cette méthode est cependant détectable par l'utilisateur lorsque celui-ci constate une multiplication anormale du nombre de secteurs défectueux.

2.4 - Virus polymorphes :

Ces virus modifient leur aspect à chaque nouvelle infection. À chaque fois qu'ils infectent un fichier, ils se cryptent différemment. Il faut donc que l'antivirus analyse la technique d'encryptage de chaque virus pour tenter de déceler, dans les fichiers contaminés, une caractéristique remarquable.
Un virus polymorphe est découpé en deux parties **:**

- Le corps principal du virus, d'une part, généralement chiffré avec une routine de chiffrement variable qui change à chaque réplication du virus. Cette partie principale présente ainsi une apparence différente à chaque fois.

- Une boucle de déchiffrement d'autre part. Elle a pour rôle de déchiffrer la partie principale du virus. Elle est également générée par le générateur de polymorphisme, comme le corps principal. Car, si cette boucle de déchiffrement était toujours la même, un antivirus pourrait essayer de la repérer elle, plutôt que le corps principal, et le travail de détection resterait simple. A l'inverse, en générant cette boucle de déchiffrement aléatoirement, le virus la rend potentiellement indétectable elle aussi.

2.5 - Virus de macros :

Ces virus s'attaquent aux macros des logiciels de la suite Office, de Microsoft (Word, Excel, ...). Ils attaquent grâce au langage VBA (Visual Basic for Applications) du même éditeur.

Avant toute chose, il convient de définir les macros. Il s'agit d'un petit programme permettant d'automatiser une série de commandes d'une application spécifique. Le pouvoir de la

macro dépend de l'application. Certaines autorisent leurs macros à accéder aux fichiers, permettant de se reproduire.

Le fonctionnement d'un virus macro est simple. Il peut agir tel un virus classique, en recherchant des fichiers cible pour les infecter. Il peut aussi infecter le modèle Normal.dot. Celui-ci est comparable au secteur d'amorçage du programme, dans le sens où il s'agit du modèle standard sur lequel repose tout document créé dans ce logiciel (sauf modèle personnel). Le modèle infecté, et donc le virus, est exécuté à chaque création de document ou d'ouverture d'un document reposant sur lui.

Certaines macros sont exécutées automatiquement lors d'une action donnée (la macro AutoExit est ainsi exécutée lorsque l'on quitte l'application, AutoClose, lorsque l'on ferme un document, ou encore AutoOpen, lorsque l'on ouvre un fichier). Il est aisé pour un virus de se répandre grâce à elles.

Les macro-virus ont d'autres possibilités. Ainsi, ils peuvent modifier les menus de l'application. Certains modifient par exemple l'option Save As (Enregistrer sous) pour sauvegarder le virus en plus du document, et ainsi se propager. D'autres modifient l'action de certains raccourcis claviers, par l'exécution du virus. Ils modifient en outre souvent le contrôle des macros dans l'application. En supprimant le menu d'accès aux macros, ou en le modifiant pour qu'il apparaisse vide, ils empêchent l'utilisateur de les détecter ou de modifier la macro virale.

Ces virus sont parfois stoppés par l'évolution des macros. Les problèmes de compatibilité induisent qu'un virus écrit pour les macros d'une ancienne version de Word ne fonctionnera peut-être plus sur une version plus récente. Ils sont néanmoins très fréquents et connaissent une propagation importante. Leur nombre avoisine les 2000, et on en découvre environ cinq(05) chaque jour. Ils peuvent causer de nombreux dégâts (jusqu'au formatage du disque dur), car le langage VBA donne une très grande liberté aux programmeurs.

Certains virus de macros infectent des fichiers exécutables, en plus des documents. Ils sont alors également des virus classiques.

2.6 -Virus flibustiers :

Ils ont pour but de désactiver l'antivirus. Ils sont rares mais diablement efficaces et dangereux, le système devenant totalement vulnérable.

2.7 - Virus compagnons :

Un virus à l'ancienne, très aisé à détecter. Sur les systèmes DOS, une priorité d'exécution est accordée aux fichiers portant l'extension .com. En créant un fichier .com portant le même nom que l'exécutable .exe, le virus est activé en premier, et peut se reproduire, avant de donner l'accès au fichier exécutable original.

2.8 - Virus crypté :

L'objectif est de crypter le code du virus à chaque duplication pour qu'il ne soit pas détecté par des outils d'analyse de code. Il est aussi possible que le programme de cryptage soit crypté.

2.9 - Virus résident :

Appelé plus communément TSR (Terminate and StayResident), un virus résident tente de se dissimuler dans la mémoire vive. Il se met en attente d'un événement du type **:** suite de caractère saisit au clavier, une heure, une date ...

2.10 - Virus parasite :

Le virus parasite copie le virus a la fin du fichier infecté. Il est exécuté par une routine de saut placé dans l'entête. Les fichiers principalement concernés sont les .com, .exe, .sys, .bin.

2.11 - Virus avec recouvrement :

Il prend la place du fichier infecté en conservant ces propriétés, taille ...

2.12 -Virus multi catégories :

Nous avons listé jusqu'ici les catégories de virus « simples ». Mais un virus peut regrouper plusieurs des caractéristiques citées. Plus il en regroupe, plus il est dangereux, et complexe à détecter.

2.13 -Vers :

Certains experts ne classent pas les vers dans les virus, tandis que d'autres les considèrent effectivement comme des dérivés. Étant donné que les vers possèdent les caractéristiques principales des virus, notamment la propagation, nous les incluons dans notre classification.

Les vers, également appelés virus de messagerie, se répandent par le courrier électronique, en profitant des failles de certains logiciels de messagerie (notamment Outlook Express, de Microsoft). Ils se copient en mémoire de l'ordinateur pour l'infecter. Et, dès lors, ils se propagent en s'envoyant eux-mêmes à tout ou partie du carnet d'adresses du logiciel de messagerie. On reçoit ainsi ce virus dans un mail d'une personne connue, ce qui diminue la méfiance. Selon leur complexité, les vers génèrent des messages et des objets distincts pour les mails par lesquels ils s'envoient.

Les vers sont plus généralement des virus réseau. Si nombre d'entre eux se propagent via les clients de messagerie, ils peuvent aussi utiliser d'autres mécanismes réseau pour se répliquer. Comme par exemple exploiter un port ouvert sur une machine, ou se propager aux machines connectées en réseau à la machine infectée, y compris en craquant les mots de passe pour s'identifier sur les machines cibles. Notons au passage que ces vers infectent aussi des machines Unix. Le premier ver était même développé pour Unix !

Leur premier effet est de saturer les réseaux, puisqu'ils les utilisent comme vecteur de propagation. La charge est exponentielle, puisque chaque ordinateur infecté permet la propagation dans plusieurs autres (parfois plusieurs centaines, si le carnet d'adresses est très fourni). Dans le cas d'un petit réseau, leur éradication est simple, il suffit d'éteindre les ordinateurs du réseau. Le problème est qu'avec l'avènement d'Internet, il est difficile d'éteindre toutes les machines connectées, ce qui rend ces virus difficilement contrôlables. Outre cet effet de saturation, qui peut aller très loin, ils sont également parfois capables d'effectuer des actions malveillantes sur les ordinateurs hôtes, comme détruire des données.

2.14 - Chevaux de Troie :

Cette dernière catégorie de logiciels malveillants n'est pas un virus, car elle n'est pas destinée à se dupliquer. Nous la détaillons succinctement tout de même, car de nombreuses personnes l'assimilent à tort aux virus.

Il s'agit de véritables bombes à retardement implantées dans un programme. Elles peuvent se déclencher à tout moment, en fonction d'un signal. Ce peut être une date précise, ou un signal externe (un message réseau envoyé par le pirate par exemple).

Les chevaux de Troie (troyens) sont une partie d'un programme, qui paraît anodin, permettant de prendre le contrôle de l'ordinateur à distance. Les dégâts causés par cette bombe peuvent même être d'ordre matériel, en modifiant par exemple le BIOS de la machine en vue entraîner une surcharge électrique.

2.15 – Les Hoax :

Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries avec des chaînes de mails. Certaines fausses alertes misent également sur l'ignorance des utilisateurs en matière d'informatique pour leur faire supprimer des éléments sains de leur système.

3 - Cycle de vie d'un virus :

Les virus informatiques suivent un cycle de vie, qui recense 7 grandes étapes :

3.1 - Création :

C'est la période durant laquelle un programmeur développe un virus aussi féroce que possible (dans la majeure partie des cas). La programmation se fait généralement en code assembleur ou Visual Basic, ou encore parfois en C ou C++.

3.2 – Gestation :

C'est le temps pendant lequel le virus s'introduit dans le système qu'il souhaiter infecter. Il y reste en sommeil.

3.3 - Reproduction (infection) :

Comme nous l'avons dit, le virus doit se reproduire. Un virus correctement conçu se reproduira un nombre important de fois avant de s'activer. C'est là le meilleur moyen de s'assurer de la pérennité d'un virus.

3.4 –Activation :

Les virus possédant une routine de destruction (portions de code destinées à causer des dégâts sur l'hôte) ne s'activent que lorsque certaines conditions sont réunies. Certains s'activent à une date précise (fixée par le développeur), d'autres possèdent un système de compte à rebours interne. L'activation peut aussi avoir lieu à distance, par le développeur. Même les virus ne possédant pas de telles routines et ne nécessitant pas de procédure d'activation spécifique peuvent causer des dommages aux systèmes en s'appropriant petit à petit l'ensemble des ressources.

3.5 –Découverte :

C'est le moment où l'utilisateur s'aperçoit que son système a des comportements étranges et soupçonne la présence de virus. Ou alors, les antivirus performants découvrent certains virus avant qu'ils aient eu le temps de faire des ravages.

3.6 – Assimilation :

Une fois la découverte faite, les développeurs de logiciels antivirus mettent à jour leur base de données virale (nous reviendrons sur cette notion) afin que les utilisateurs puissent détecter la présence de virus sur leur ordinateur. Ils développent également le correctif (ou antidote) permettant d'éradiquer le virus (si cela est possible).

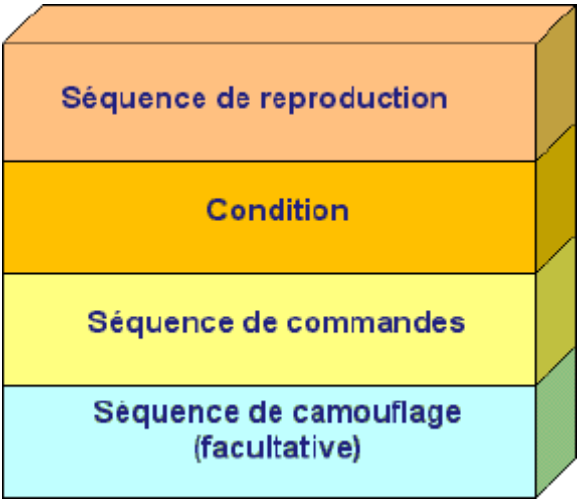
3.7 –Élimination :

C'est la mort du virus. Tout au moins, c'est la mort de l'exemplaire du virus sur un poste utilisateur. C'est le moment où l'antivirus ayant découvert le virus propose à l'utilisateur de le supprimer. Même si de nombreux virus connus depuis des années ne sont pas complètement annihilés, ils ont cessé de constituer une menace sérieuse car ils sont découverts très rapidement. Dans les faits, rares sont les virus ayant complètement disparu.

2.7 - Structure des virus :

Un virus se compose de 3 fonctionnalités principales et d'une quatrième optionnelle (mais de plus en plus présente dans les virus afin d'en améliorer l'efficacité), comme le montre la Figure suivante :

- **Séquence de reproduction ;**
- **Condition ;**
- **Séquence de commandes ;**
- **Séquence de camouflage.**



4 - La propagation des virus :

Il existe de nombreux supports de propagation des virus. D'autant plus avec l'explosion de l'Internet au cours de la dernière décennie, qui fournit la plus grosse autoroute de circulation pour les virus.

Au départ, les supports amovibles constituaient les moyens de propagation des virus. Les disquettes dans un premier temps, puis les Cd gravés, les disques durs externes, et pourquoi pas aujourd'hui la clé USB. Si le virus se trouve dans un fichier qu'une personne souhaite transférer sur un autre ordinateur par l'intermédiaire d'un support amovible, il pourra infecter l'ordinateur de destination.

Les réseaux locaux domestiques, et plus encore ceux des entreprises constituent également un vecteur de propagation important. Les ordinateurs étant tous connectés les uns aux autres, il est facile d'utiliser le réseau pour répandre le virus sur toutes les machines.

En ce qui concerne l'Internet, les mails contenant le virus en pièces jointes sont un grand classique. Par plusieurs systèmes plus ou moins subtiles, le concepteur du virus fait en sorte de pousser l'utilisateur qui reçoit le mail à exécuter la pièce jointe

pour infecter l'ordinateur. Le virus peut se débrouiller pour s'envoyer à toutes les personnes du carnet d'adresse de la première victime et ainsi de suite. Et se propager de manière exponentielle.

Enfin, il y a la propagation due au téléchargement. Soit directement en téléchargeant sur un site un fichier infecté. Soit sur les réseaux de peer-to-peer. PLAGIAT

5 -Les motivations et les causes des virus :

Les motivations des développeurs de virus trouvent plusieurs sources, et notamment :

5.1- Vengeance :

Un employé ayant été licencié par son entreprise peut vouloir se venger. Il écrira pour cela un virus pour effacer toute les bases de données de l'entreprise ou juste les modifier de façon à faire perdre de l'argent à son ancien employeur. Il peut aussi ralentir le réseau de l'entreprise et bien d'autres choses encore.

5.2 - Malveillance, amusement ou compétition :

L'écriture d'un virus peut aussi avoir comme but la pure malveillance d'un utilisateur ou son amusement. En effet, pour certaines personnes, créer des virus est un jeu, où il faut faire toujours mieux que le concurrent, et rivaliser d'ingéniosité pour créer "LE" virus complètement invisible et dévastateur. Ou paralyser l'Internet sur le plus large périmètre possible...

5.3 -Curiosité :

Cette motivation est sûrement la plus courante. Beaucoup de développeurs de virus avancent que la curiosité, l'envie de découvrir et d'apprendre, est le principal moteur de leurs actes. Mais cela peut aussi devenir du voyeurisme. Certaines personnes peuvent aussi être curieuse de connaître des informations secrètes et développer ainsi un virus qui serait capable de pénétrer certains systèmes informatiques sécurisés, et ce pour avoir accès aux informations secrètes contenues dans ces systèmes. Par exemple, un utilisateur voulant avoir le mot de

passe du compte UNIX d'un autre utilisateur pour avoir accès à ses données et pouvoir les modifier par la suite, pourra créer un virus qui mettra tous les mots tapés au clavier dans un fichier, y compris les mots de passe. Il n'aura ensuite plus qu'à piocher dans ce fichier pour repérer le mot de passe.

5.4 - Le pouvoir et l'argent :

Il n'est pas très difficile d'imaginer que certaines personnes puissent mettre au point des virus qui pourraient dérégler les comportements des ordinateurs d'une banque dans le but de récupérer de l'argent suite à des versements fictifs. Ou récupérer des informations secrètes d'une grande société dans le but de les vendre à la concurrence.

II- L'ANTIVIRUS :

L'antivirus sont des programmes capables de détecter la présence de virus sur un ordinateur, ainsi que de nettoyer celui-ci dans la mesure du possible si jamais un ou des virus sont trouvés. Nettoyer signifie supprimer le virus du fichier sans l'endommager. Mais parfois, ce nettoyage simple n'est pas possible.

1 - Les types d'antivirus :

On dénombre bien sûr deux types d'antivirus. Les scanners, exécutés à la demande (On-Demand Scanners), et les moniteurs, toujours actifs à l'arrière-plan (On-Access Scanners). Nous ne nous attarderons pas sur les scanners à la demande, qui utilisent les méthodes déjà expliquées pour chercher des virus dans tous les fichiers des supports accessibles (disques durs, CD-Roms, disquettes).

Les moniteurs de comportement observent l'ordinateur en arrière-plan (en permanence, de manière transparente), pour détecter toute activité de type virale. Ils peuvent entre autres détecter les tentatives d'ouverture en écriture des fichiers exécutables, les tentatives d'écriture sur les secteurs d'amorçage, ou les tentatives d'un exécutable à devenir résident.

Pour détecter ces tentatives, les logiciels antivirus attrapent les principales interruptions de l'ordinateur, en les remplaçant par l'adresse de leur code. Ainsi, dès qu'un virus tente d'écrire sur le secteur d'amorçage ou sur le disque, c'est l'antivirus qui est d'abord appelé, et non le système directement. L'antivirus peut alors éliminer le virus, s'il le détecte.

Un moniteur résident analyse ainsi toute l'activité du PC, que ce soit les fichiers entrants et sortants de l'ordinateur, le logiciel de messagerie électronique, les exécutables, et même souvent tous les fichiers accédés en lecture ou en écriture. Les moniteurs actuels sont également capables de parcourir les fichiers compressés auquel on accède, afin de vérifier qu'aucun des fichiers qu'ils contiennent ne promène de virus.

Un tel moniteur est extrêmement important, surtout pour les machines connectées à un réseau, et a fortiori à l'Internet, ce qui est de plus en plus fréquent.

Bien sûr, les détracteurs de ce genre de logiciel arguent qu'ils ralentissent la machine, diminuent les performances. C'est une évidence, dans la mesure où ils analysent de nombreux événements du système. Néanmoins, sur des machines récentes, c'est beaucoup moins gênant pour l'utilisateur. Et c'est le prix à payer pour une tranquillité plus importante.

2 - Signature virale :

Comme nous l'avons vu, les virus infectant des applications, copient leur code dans ces programmes. Et les virus sont programmés pour ne pas infecter plusieurs fois le même fichier. Dès lors, ils intègrent dans l'application infectée une signature virale, c'est-à-dire une suite d'octets significative, qui leur permet de vérifier si tel ou tel programme est déjà infecté.

La méthode de base utilisée par l'antivirus est donc de détecter cette signature propre à chaque virus. Évidemment, cette méthode n'est fiable que si l'antivirus possède une base virale à jour, contenant les signatures de tous les virus connus. Néanmoins, ce mécanisme ne permet pas la détection des virus « inconnus », c'est à dire n'ayant pas encore été répertoriés par les

éditeurs. En outre, n'oublions pas que les virus polymorphes, dont nous avons déjà parlé, sont capables de se camoufler, c'est-à-dire de rendre leur signature indétectable (en la cryptant et en la modifiant à chaque copie).

3 - Contrôleur d'intégrité des programmes :

Puisque les virus modifient les programmes qu'ils infectent, certains antivirus utilisent un contrôleur d'intégrité pour vérifier si les fichiers de la machine ont été modifiés. Ainsi, une base de données est construite, qui contient des détails sur les fichiers exécutables du système, comme leur taille ou leur date de modification, et éventuellement un checksum. Dès lors, si une de ces caractéristiques change pour un exécutable, l'antivirus s'en aperçoit.

4 - Analyse heuristique :

L'analyse heuristique est relative à la recherche de code informatique correspondant à des fonctions de virus. C'est-à-dire qu'elle est vouée à découvrir des virus encore inconnus. L'analyse heuristique est passive. Elle considère le code comme une simple donnée, et n'autorise jamais son exécution. Un analyseur heuristique recherche du code dont l'action pourrait s'avérer suspecte. En l'occurrence, il ne cherche pas des séquences fixes d'instructions spécifiques à un virus, mais un type d'instruction. Par exemple, des instructions visant la modification d'un fichier.

Cette méthode se dirige vers une démarche « intelligente » de recherche de virus. Cela dit, elle est loin d'être totalement efficace. Elle fonctionne bien pour les macros virus, moins bien pour les autres. Les plus sensibles des antivirus heuristiques produisent nombre de fausses alertes, et les moins agressifs rateront à coup sûr de véritables virus.

5 - Analyse spectrale :

L'analyse spectrale repose sur le postulat que tout code généré automatiquement contiendra des signes révélateurs du compilateur utilisé. De même, on part du principe qu'il est impossible de retrouver dans un vrai programme exécutable compilé certaines séquences de code. L'analyse spectrale vise donc elle aussi à repérer les virus polymorphes ou inconnus. Lorsqu'un virus polymorphe crypte son code, la séquence en résultant contient certaines associations d'instructions que l'on ne trouverait pas dans un vrai programme. C'est ce que l'analyse spectrale tente de détecter. Par exemple, si dans un programme exécutable, l'antivirus trouve une instruction de lecture d'un octet au-delà de la taille limite de la mémoire, on sera probablement en présence de code crypté, donc d'un virus polymorphe.

6- Désinfestation d'un PC :

Une fois un virus détecté, il faut le supprimer. Mais il n'est pas toujours simple de supprimer un virus sans endommager le programme original. En effet, certains virus détruisent une partie du programme sain lors de leur duplication. Il ne reste plus alors qu'à détruire purement et simplement le fichier infecté. Dans les autres cas, la suppression du virus n'est pas forcément évidente non plus. Il s'agit d'abord de découvrir très précisément où est localisé le virus dans le fichier, sachant qu'il peut être composé de plusieurs parties. Il faut ensuite supprimer ces octets infectés, et récupérer la partie du programme dont le virus avait pris la place, afin de la restaurer. Toutes ces manipulations nécessitent bien sûr une parfaite connaissance du virus et de son mode opératoire. C'est à cela que servent les fichiers de signatures de l'antivirus, régulièrement remis à jour. Il faut non seulement pouvoir détecter le virus, mais aussi savoir où il cache la portion de code dont il a pris la place.

Certains virus plus complexes nécessitent un outil de suppression pour éliminer toutes les manifestations de la bête. Ils sont également utilisés pour les virus à grande échelle, lorsque les utilisateurs n'ont pas d'antivirus. Par exemple, pour le ver Blaster, un programme de fix a été proposé par l'éditeur Symantec, qui n'avait pas besoin d'antivirus pour s'exécuter.

Il est entendu qu'aucun antivirus ne détecte tous les virus. Lorsqu'un nouveau virus est détecté, et qu'une mise à jour est disponible, même en quelques heures, il faut la télécharger, sans quoi l'antivirus ne fonctionne pas. À part les quelques techniques de découverte des virus inconnus, qui, nous l'avons vu, ne sont pas totalement au point.

7- Prévention :

Comme il a été souligné précédemment, il existe un grand nombre de virus. De ce fait, chaque utilisateur se doit d'avoir un comportement préventif, afin de minimiser les risques d'infection. Donc, pour minimiser les infections, il est nécessaire d'avoir une conduite préventive ainsi que de posséder des logiciels prévenant les infections, voire par les logiciels permettant la désinfection des systèmes.

La prévention provient essentiellement de l'attitude des utilisateurs, qui représente la première ligne de défense contre les infections. Les utilisateurs devraient respecter certaines règles, afin d'éviter tout risque d'infection, tel que :

- Se méfier d'un nom de fichier attaché ou d'un sujet d'e-mail trop attractif ;
- Ne jamais ouvrir un fichier joint avec une extension (.exe, .com, .bat, .vbs, .pif, .ovl ou .scr);
- Se méfier des documents Word (.doc), Excel (.xls) ou PowerPoint (.pps) contenant des macros en Visual Basic ;
- Ne jamais ouvrir un fichier contenant une double extension, comme " TrucMuche.GIF.VBS ", qui sont des astuces utilisées pour cacher la vraie identité d'un fichier infecté ;

- Ne jamais faire confiance à l'expéditeur, même si c'est une personne connue. En effet, certains vers se servent des carnets d'adresses d'ordinateur infecté pour se propager ;
- Ne pas insérer de disquettes sans en connaître la provenance ;
- Sauvegarder régulièrement ses fichiers importants, car même avec la plus extrême vigilance, le pire peut arriver.
- Installer un antivirus ;
- Vérifier la provenance des fichiers téléchargés sur Internet (vérifier avec l'antivirus qu'ils ne sont pas infectés) ;
- Supprimer tous les e-mails non sollicités. (ex. : SPAM) ;
- Mettre à jour régulièrement les définitions de virus.

III- SAUVEGARDE DES DONNÉES :

1- Définition :

En informatique, la sauvegarde (aussi appelée **backup**) consiste à répliquer des données à un autre emplacement ou sur un autre support, dans le but de les mettre en sécurité.

2 - Objectifs de la sauvegarde :

La perte de données stockées sur un ordinateur professionnel peut avoir des conséquences dramatiques pour l'entreprise. Vols, sinistres, défaillance informatique, piratage : l'origine des pertes est multiple. C'est pourquoi les solutions de sauvegardes de données sont indispensables.

Ne pas sauvegarder vos données peut s'avérer risquer si celles-ci sont vitales.

La sauvegarde des données préserve l'activité de l'entreprise, notamment en cas de défaillance du système informatique. L'entreprise peut faire face à plusieurs types de risques qui mettent en danger ses données **:**

- Risques humains **:**La perte ou le vol d'un appareil dont les données sont liées à celles de l'entreprise, une mauvaise manipulation entraînant l'effacement de données sensibles, piratage des données...,

- Risques liés à l'environnement **:** Perte de données suite à un incendie dans les locaux de l'entreprise, catastrophes (incendies, inondations...),
- Risques liés aux dysfonctionnements matériels **:**Perte d'un serveur par exemple.

En cas de pertes de données, l'impact financier peut être notable pour l'entreprise en raison de la disparition de fichiers ou d'applications sensibles (base de données clients, rapports financiers, etc.), ou de la perte de temps engendrée par la remise en ligne de ces données.

3-Types de sauvegarde :

Il existe trois grands types de sauvegarde **:**

- La sauvegarde **complète ;**
- La sauvegarde **incrémentale ;**
- La sauvegarde **différentielle.**

a) Sauvegarde complète :

Il s'agit d'une sauvegarde de tous les fichiers, effectuée à l'instant T. Dans votre système d'exploitation, c'est (en gros) comme si vous faisiez un copier-coller de vos données depuis votre ordinateur vers un disque dur externe ou une clé USB. Lorsque vous souhaitez effectuer une restauration de vos données, vous prenez la sauvegarde la plus récente (effectuée le jour J) et tous les fichiers sont restaurés dans leur état au jour où ils ont été sauvegardés (jour J).

Lorsque vous effectuez une sauvegarde complète, un marqueur est placé à 0 sur l'ensemble des fichiers.

b) Sauvegarde différentielle :

Une première sauvegarde complète est effectuée le jour J. La sauvegarde différentielle, effectuée par exemple le jour J+1, ne contiendra que les fichiers modifiés par rapport au jour J. Lorsqu'un fichier est modifié, son marqueur passe à 1 et il sera

sauvegardé indéfiniment tant qu'une nouvelle sauvegarde complète n'aura pas été effectuée.

Pour restaurer des données au jour J+5 par exemple, il conviendra de disposer de la sauvegarde complète (jour J) et de la sauvegarde du jour J+5, qui contiendra l'ensemble des fichiers ayant été modifiés au moins une fois depuis la sauvegarde complète.

c) Sauvegarde incrémentale :

La sauvegarde incrémentielle ou incrémentale fonctionne sur un principe différent. Une première sauvegarde complète est effectuée le jour J.
Le jour J+1, on réalise une sauvegarde différentielle par rapport au jour J (comprenant les fichiers modifiés uniquement entre les jours J et J+1).

Le jour J+2, on réalise une sauvegarde différentielle par rapport au jour J+1 (comprenant les fichiers modifiés uniquement entre les jours J+1 et J+2).

Et ainsi de suite ... Lorsqu'un fichier est modifié, son marqueur passe à 1. La sauvegarde sauvegardera le fichier modifié, qui aura son marqueur qui passera à 0 jusqu'à la prochaine modification, et ainsi de suite.

L'inconvénient de ce type de sauvegarde provient de la restauration **:** Pour restaurer des données sauvegardées à J+5 par exemple, il faudra récupérer la sauvegarde du jour J, mais aussi celles des jours J+1, J+2, J+3, J+4 et J+5.

4- Que sauvegarder ?

Les logiciels, on peut toujours les réinstaller. En priorité, il faut sauvegarder **:**

- ✓ **Les fichiers essentiels**

  - Les documents de gestion (comptabilité…) ;
  - Bureautique (word, excel, Access etc.)

- Artistiques (dessins, photos, musiques etc.…) ;
- Courriers, carnet d'adresses.

✓ Les fichiers de configuration **:** Ils contiennent les paramètres de fonctionnement de vos logiciels.

5 - Les différents supports de sauvegarde :

Il faudra considérer la taille du support (pour qu'il puisse recevoir l'intégralité des données à sauvegarder) et la simplicité pour réaliser la sauvegarde (pour que l'opération ne soit pas trop "contraignante") ainsi que la fiabilité du support (pour ne pas risquer une perte de données).

Parmi les supports disponibles, on peut citer **:**

- Le disque dur ;
- Le CD-ROM ou DVD-ROM ;
- La clé USB
- La sauvegarde réseau ;
- La sauvegarde sur Internet ;
- La bande magnétique.

a) Le disque dur :

C'est le moyen de sauvegarde le plus courant. On peut considérer différents niveaux de sauvegarde suivant son équipement.

Scinder le disque dur de son ordinateur en plusieurs volumes (le partitionner) et réserver une de ces partitions pour la sauvegarde est la méthode la moins coûteuse. Si vous possédez une machine de marque, il est même possible que son constructeur ait déjà réalisé ce découpage. Sinon, avec un PC sous Vista, vous pouvez le faire vous-même à l'aide de l'outil **Gestion des disques** (un tutoriel est disponible ici).

Avantages

✓ Partitionnement réalisable immédiatement sans perte de données ;
✓ Certains PC de marque sont déjà partitionnés.

Inconvénient

- ✓ En cas de panne du disque dur, fort risque de perdre toutes ses données (originaux et sauvegardes).

b) Un support à mémoire flash : clé USB, carte mémoire :

Avec une capacité allant jusqu'à 64 Go (et bientôt davantage !), les clés à mémoire flash offrent un espace très confortable pour vos sauvegardes. Leur petit format est pratique, même si c'est aussi un défaut (risque de perte). Mais pour éviter tout incident irréversible, ne succombez pas aux sirènes du *lowcost* et préférez les modèles un peu plus chers : ceux à bas prix sont réputés pour leur manque de fiabilité.

Avantages

- ✓ Mise en œuvre rapide
- ✓ Petite taille et grande capacité

Inconvénients

- ✓ Vitesse d'écriture décevante sur certains modèles
- ✓ Se perd facilement

c) Un disque optique : CD, DVD :

Aujourd'hui, avec l'accroissement fantastique de la capacité des disques durs, sauvegarder sur DVD promet d'être fastidieux, à moins de ne préserver que des fichiers vraiment essentiels. Passer au Blu-ray permet de ne plus trop se poser de questions sur la capacité (jusqu'à 50 Go, et des versions de plusieurs centaines de giga-octets sont en cours de développement). Mais il faut y mettre le prix : 10 euros pour un Blu-ray vierge de 25 Go (et non réinscriptible), et près de 200 euros pour un graveur adéquat.

Avantage

- ✓ Faible prix des CD et DVD vierges

Inconvénients

- ✓ Fragilité ;
- ✓ Pérennité aléatoire ;
- ✓ Capacité pas toujours adaptée ;
- ✓ Lenteur relative des gravures.

d) Un disque dur externe :

Prix en baisse, capacités en hausse, extrême simplicité d'installation et d'usage : les disques externes sont un support de choix pour la sauvegarde. Mais un tel support n'est pas infaillible : utilisez-le avec précaution, ne le transportez pas trop souvent, évitez les chocs. Attention : il arrive qu'un disque amovible ayant reçu un choc semble continuer à fonctionner normalement en apparence… jusqu'au jour où vous voulez accéder aux données se trouvant sur les portions endommagées. Les possesseurs de Mac devront peut-être reformater leur disque externe en FAT32, format reconnu par les Mac et PC, contrairement au format NTFS que les Mac (sous OS X) savent uniquement lire, par défaut.

Avantages

- ✓ Prix (au gigaoctet) de plus en plus bas
- ✓ Capacité très importante
- ✓ Utilisation très simple

Inconvénient

- ✓ Fragilité relative

e) Un disque réseau (NAS) :

Cette variété de disque externe peut être partagée, sur un réseau, entre plusieurs ordinateurs et peut donc recevoir les sauvegardes de différents utilisateurs. Mais sa mise en œuvre est plus complexe que celle d'un disque externe traditionnel. De plus, les vitesses de transfert sont généralement bridées, soit au niveau du NAS, soit au niveau du routeur ou de la box, par l'emploi de prises réseau 100 Mbit/s. Ce qui donne au mieux 10 Mo/s en lecture comme en écriture, contre 30 Mo/s en USB et parfois

plus de 100 Mo/s avec des disques internes. À installer en connaissance de cause.

Avantages

- ✓ Partageable entre plusieurs ordinateurs
- ✓ Fonctionne en permanence

Inconvénients :

- ✓ Mise en œuvre assez complexe
- ✓ Vitesse de transfert limitée

f) Un espace de stockage en ligne :

On peut sauvegarder sans connecter de matériel à son PC, mais en transférant ses données par Internet sur un disque distant. La plupart des FAI mettent à disposition de leurs clients un espace de stockage, mais il est souvent limité et les données stockées ne sont pas garanties contre les destructions accidentelles. Mieux vaut exploiter un serveur FTP ou utiliser un service dédié comme Carbonite (décrit dans ce guide), Neobe ou Windows Live Skydrive. Mais il faut faire confiance au prestataire qui stocke vos fichiers (confidentialité, robustesse des serveurs de stockage) et disposer d'une bonne connexion à Internet (au moins 500 kbit/s en débit montant).

Avantages

- ✓ Aucun matériel nécessaire
- ✓ Données préservées en cas de sinistre sur l'ordinateur

Inconvénients :

- ✓ Sauvegardes lentes et dépendantes de la connexion à Internet
- ✓ Il faut faire confiance au prestataire

g) Le système Raid :

Pour les professionnels : le système Raid est une bonne solution **:** voici quelques explications. La technologie RAID permet de constituer une unité de stockage à partir de plusieurs disques durs.

L'unité ainsi créée (appelée grappe) a donc une grande tolérance aux pannes (haute disponibilité), ou bien une plus grande capacité/vitesse d'écriture. La répartition des données sur plusieurs disques durs permet donc d'en augmenter la sécurité et de fiabiliser les services associés.

Les disques assemblés selon la technologie RAID peuvent être utilisés de différentes façons, appelées Niveaux RAID. Ils en existent cinq(5), auxquels ont été ajoutés les niveaux 0 et six (6).

Chacun de ces niveaux constitue un mode d'utilisation de la grappe, en fonction : des performances, du coût et des accès disques.

Les solutions RAID généralement retenues sont le RAID de niveau 1 et le RAID de niveau 5. Le choix d'une solution RAID est lié à trois critères :

- ✓ La sécurité **:** RAID 1 et 5 offrent tous les deux un niveau de sécurité élevé
- ✓ Les performances **:** RAID 1 offre de meilleures performances que RAID 5 en lecture, mais souffre lors d'importantes opérations d'écriture.
- ✓ Le coût : le coût est directement lié à la capacité de stockage devant être mise en œuvre pour avoir une certaine capacité effective. La solution RAID 5 offre un volume utile représentant 80 à 90% du volume alloué (le reste servant au contrôle d'erreur).
  La solution RAID 1 n'offre par contre qu'un volume disponible représentant 50 % du volume total (étant donné que les informations sont dupliquées).
  Il existe plusieurs façons différentes de mettre en place une solution RAID sur un serveur : de façon logicielle et de façon matérielle.

6 - Les outils de sauvegarde :

a) Utilitaire de sauvegarde Windows :

Sacher que Windows intègre depuis Windows 98, un utilitaire de sauvegarde :

Démarrer/Tous les programmes/accessoires/outil système/utilitaires de sauvegarde. On peut choisir les fichiers à sauvegarder ou l'état du système.
C'est intéressant à faire avant d'installer des nouveaux pilotes par exemple.

b) Logiciels de "sauvegarde" :

Il existe aussi des logiciels de sauvegardes très puissants comme Norton Ghost, qui permet de créer une image du disque dur, un instantané de votre configuration sous la forme d'un fichier image, cela permet de gagner un temps précieux, plus besoin de formater ou de réinstaller Windows.

- ✓ Synback
- ✓ Cobian Backup
- ✓ Acronis True Image Home
- ✓ MozBackup

c) Sauvegarde en ligne :

Il existe aussi la solution sauvegarde en ligne. En apprenant à se servir d'un logiciel ftp et puisqu'on bénéficie d'un espace mis à notre disposition par notre fournisseur d'accès (100 à 150 Mo) pour nos pages perso, pourquoi ne pas l'utiliser ?

EXERCICES PRATIQUES :

Sauvegarder Windows Server 2008

I- PRÉSENTATION :

Il existe plusieurs moyens de sauvegarder un système entier comme sur un DVD, un espace du disque du local ou distant mais Windows 2008 server dispose de son propre système de sauvegarde. Nous allons apprendre à l'utiliser dans ce tutoriel.

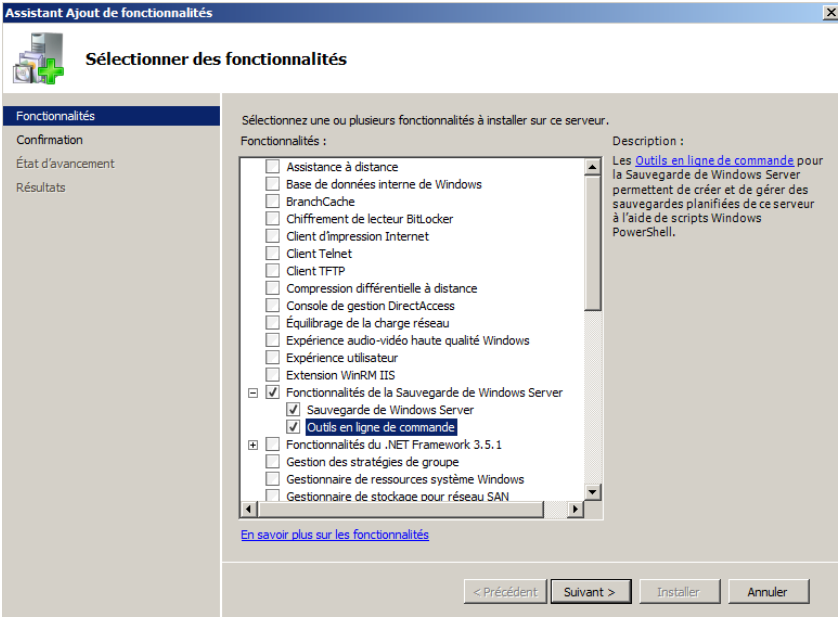
Il faut savoir qu'il existe plusieurs façons d'utiliser le gestionnaire de sauvegarde de Windows 2008 server. Celui-ci gère en effet la sauvegarde locale et distante, il peut effectuer une sauvegarde ponctuelle ou régulière et peut faire une sauvegarde de tout le serveur ou seulement des volumes désignés.

Une sauvegarde peut être faite sur un disque local, un DVD ou un dossier partagé distant.

II-INSTALLATION DU SERVICE DE SAUVEGARDE :

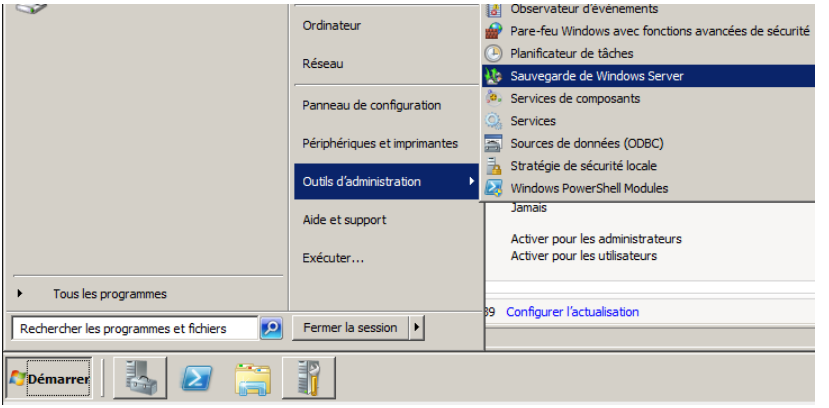
Dans un premier temps, il faut installer une fonctionnalité dans notre Windows 2008 server.
Pour cela, rendez-vous fans « **Démarrer**«, « **Outils d'administration** » puis « **Gestionnaire de serveur**«. Une nouvelle fenêtre apparait, c'est la console MMC gestionnaire de serveur.

Dans la colonne de gauche, rendez-vous dans « **Fonctionnalités** » puis dans la colonne de droite allez dans « **Ajouter une fonctionnalité** « .Vous aurez alors une liste de fonctionnalités que vous pourrez ajouter. Sélectionnons celles qui nous intéressent comme suivant **:**



L'outil en ligne de commande va nous permettre de gérer les sauvegardes par la ligne de commande, ce n'est pas une fonctionnalité obligatoire pour la sauvegarde de notre serveur mais nous apprendrons plus tard à le faire en ligne de commande. Cliquez ensuite sur « **Suivant** » puis sur « **Installer**«.

Notre service de sauvegarde est maintenant installé ! Nous allons pouvoir faire notre sauvegarde en nous rendant dans « **Démarrer** », « **Outils d'administration** » puis dans « **Sauvegarde de Windows Server**« .



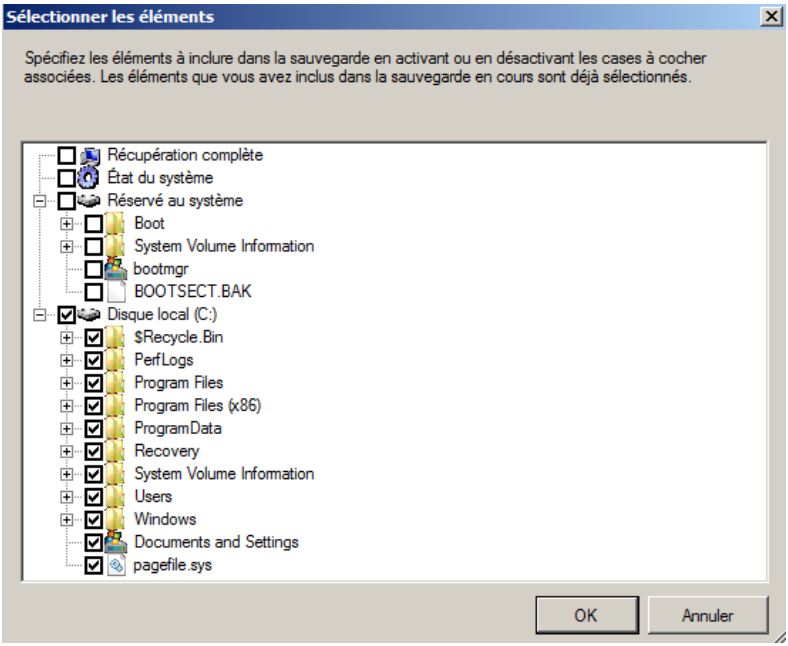
Nous pouvons alors soit faire une sauvegarde ponctuelle, soit planifier des sauvegardes régulières.

1- Faire une sauvegarde ponctuelle :

Nous allons commencer pour faire une sauvegarde ponctuelle (unique). Il nous faut cliquer sur « **Sauvegarde unique** » dans le panneau de droite de la fenêtre « **Sauvegarde de Windows Server**«.

Deux choix s'offrent à nous, l'utilisation des même paramètres de sauvegarde que les sauvegardes planifiées (grisé si vous n'en avez jamais fait) ou « **Autre options**«. Nous sommes ici contraints de choisir « Autres options » puis de cliquer sur « **Suivant**«.

A nouveaux deux options s'offrent à nous. Cela dépend du type de sauvegarde que vous souhaitez faire. Si vous choisissez « **Personnalisé** » vous trouverez une fenêtre ou il faudra cliquer sur « **Ajouter des éléments** » pour sélectionnez les volumes ou dossiers que vous souhaitez sauvegarder, comme suivant **:**



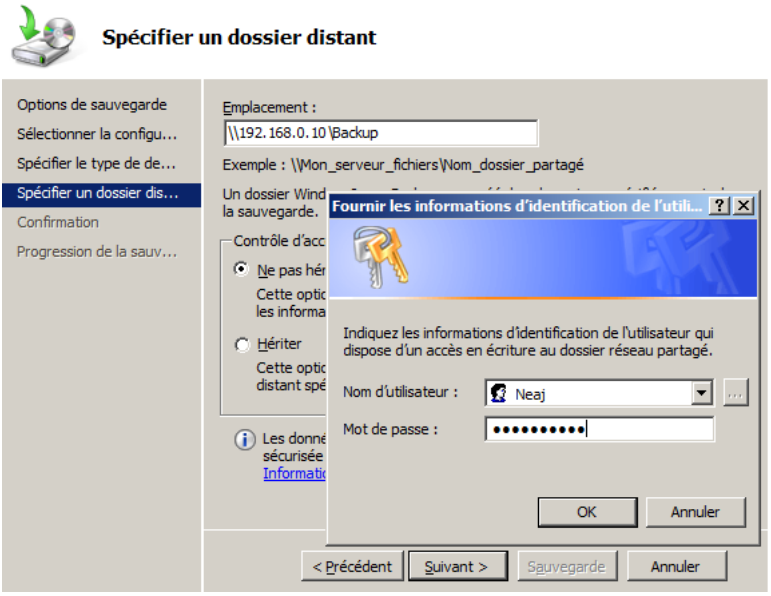
Dans paramètres avancés, vous trouvez aussi des options pour exclure certains fichiers ou dossiers par type (par exemple) ainsi que les paramètres VSS.

Si vous choisissez « **Serveur entier**«, la sauvegarde portera sur l'intégralité des volumes et des dossiers de votre serveur.
Quelque que soit l'option choisie, nous auront ensuite à choisir le type de stockage pour notre sauvegarde. Il peut s'agir d'un lecteur local (DVD, disque dur..) ou distant (un autre serveur..). Pour choisir le lecteur local comme type de stockage, il faut bien sur disposer d'un disque dur vide ou d'un DVD vierge pour pouvoir y mettre notre backup.

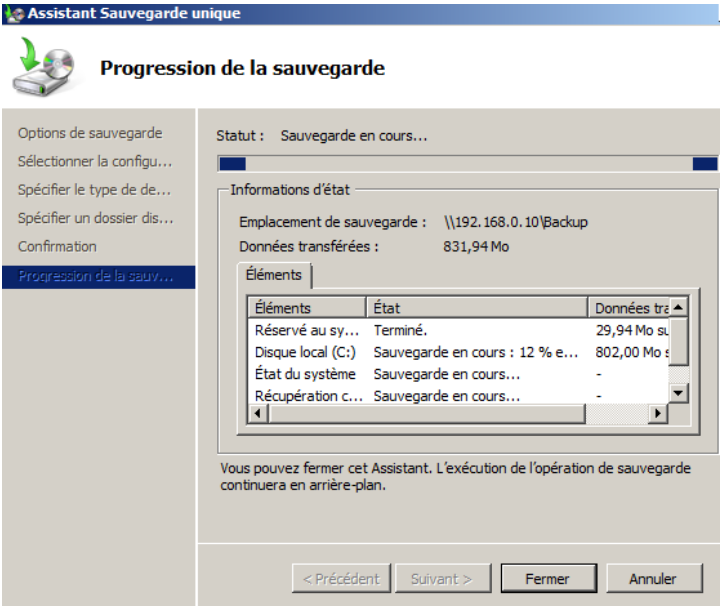
Ici nous allons choisir un dossier partagé distant, assurez-vous d'avoir un dossier partagé sur une autre machine et procurez-vous son nom d'hôte ou son IP pour pouvoir la joindre avec notre Windows 2008 server. Sélectionnez ensuite « **Dossier partagé distant**«. Pensez également à vérifier les droits d'écriture sur votre partage !

Vous aurez ensuite à entrer le chemin vers votre dossier partagé distant afin que la sauvegarde s'effectue dans ce dossier. Il faut ensuite gérer le contrôle d'accès au Backup. Soit on donne la permission d'accès à tous les utilisateurs ayant accès au dossier partagé distant (« **Hériter**«), soit on donne accès uniquement à l'utilisateur que nous spécifions par la suite (« **Ne pas hériter**«)

Il vous faudra ensuite entrer les identifiants de l'utilisateur qui aura accès au dossier partagé distant si vous avez sélectionné « **Ne pas hériter**« :



Pour finir, il nous faut cliquer sur « **Sauvegarder** » pour lancer la sauvegarde

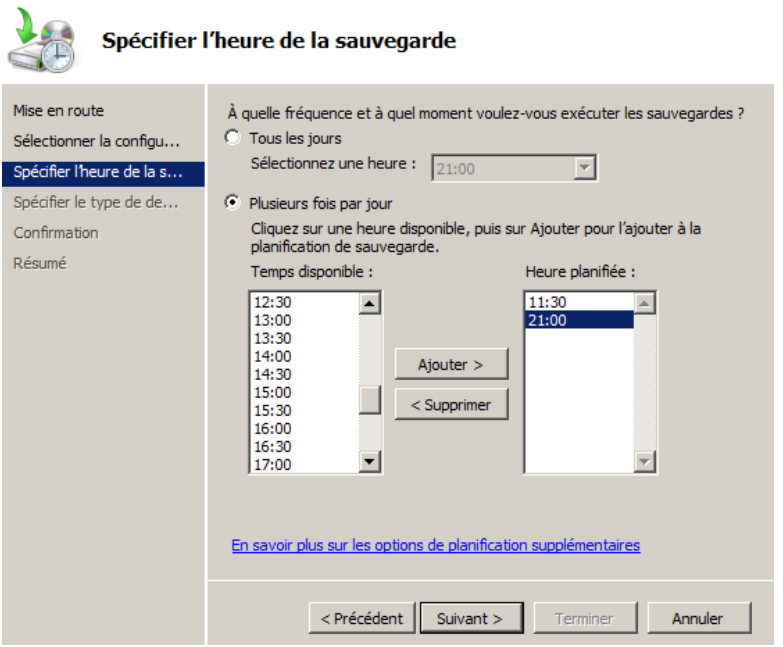


Une fois celle-ci effectuée, vous pourrez retrouver votre Backup dans le dossier partagé.

2-Configurer une sauvegarde régulière

Dans la fenêtre de Sauvegarde de Windows Server, il faut cliquer sur « **Planification de sauvegarde** » puis sur « **Suivant** » .

Il faut à nouveau choisir entre « **Serveur entier** » ou « **Personnalisé**«. Puis nous arrivons sur cette fenêtre :



Vous pouvez alors choisir entre une sauvegarde tous les jours à la même heure, ou à plusieurs heures dans la journée. Pour la deuxième option il faut sélectionner l'heure voulue puis cliquer sur le bouton « **Ajouter** > » pour paramétrer une sauvegarde quotidienne à cette heure ou « < **Supprimer** » pour l'enlever.

La suite de la procédure est la même que pour une sauvegarde unique.

3- Sauvegarde en ligne de commande :

Il est possible de faire des sauvegardes par la ligne de commande. Cela est uniquement possible si vous avez cocher l'outils de sauvegarde en ligne de commande lors de l'ajout des fonctionnalités. Cela active l'outilwbadmin qui gère la sauvegarde en ligne de commande. Wbadmin enregistre l'état du système (AD, sysvol et registre/fichiers d'amorçage).

- **wbadminstart backup** : indique que nous allons exécuter une sauvegarde

- **backupTarget:\\192.168.0.10\Backup** : indique l'endroit où nous allons sauvegarder nos informations. Ici il s'agit d'un répertoire distant mais cela aurait très bien pu être un lecteur ou un volume local (exemple D:).

- **include:C:,H:** : indique les volumes que nous voulons sauvegarder

- **-vssFull** : le service VSS sert à gérer la sauvegarde des fichiers en cours (ouverts), le vssFull sauvegarde les fichiers dans leur états actuels (avec les modifications récentes). Si cette option n'est pas précisée, c'est le vssCopy qui sera actif. Alors, les fichiers seront sauvegarder dans leurs états non modifiés. C'est à dire qu'un fichier qui aura été modifié mais pas encore sauvegardé par l'utilisateur ne sera pas sauvegardé avec ses nouvelles modifications.

- **-exclude:H:\dossierTmp*** : nous permet d'exclure un fichier ou un dossier de la sauvegarde bien que son volume parent ai été spécifié.

Il existe d'autres options d'exécution de la commande wbadmin, pour voir toutes celles qui existent, utilisé la commande **:**
wbadminstart backup /?

III- SAUVEGARDE DE L'ÉTAT DU SYSTÈME :

1- Le Journal d'événements :

Les journaux d'évènements Windows existent depuis la première version de Windows NT, en 1993, toutes les versions de Windows, depuis, étant basées sur Windows NT.

Les journaux des évènements sont des fichiers spéciaux qui enregistrent les évènements significatifs sur votre ordinateur, tels que l'ouverture d'une session sur l'ordinateur par un utilisateur ou lorsqu'un programme rencontre une erreur. À chaque occurrence de ces types d'évènements, Windows enregistre l'évènement dans un journal des évènements que vous pouvez consulter à l'aide de l'Observateur d'évènements. Les utilisateurs avancés peuvent utiliser les informations contenues dans les journaux des évènements pour résoudre des problèmes dans Windows et d'autres programmes.
L'Observateur d'évènements assure le suivi des informations dans plusieurs journaux différents. Les journaux Windows comprennent **:**

- **Les évènements d'application (programme).** Les évènements sont classés en « erreur », « avertissement » ou « informations » selon la gravité de l'évènement. Une « erreur » indique un problème important, comme la perte de données. Un « avertissement » est un évènement qui n'est pas nécessairement significatif mais qui peut annoncer des problèmes ultérieurs. Un évènement d' « informations » décrit le bon fonctionnement d'un programme, d'un pilote ou d'un service.

- **Les évènements liés à la sécurité.** Ces évènements sont appelés des audits et sont considérés comme réussis ou non, selon que l'évènement, comme un utilisateur cherchant à ouvrir une session Windows, aboutit ou non.

- **Les évènements système.**

  Ces évènements sont enregistrés par Windows et les services système de Windows, et sont classés comme erreur, avertissement ou informations.

- **Les évènements de configuration.**

  Les ordinateurs configurés comme contrôleurs de domaine affichent des journaux supplémentaires à cet emplacement.

- **Les évènements transférés.**

  Ces évènements sont transférés à ce journal par d'autres ordinateurs.

2- Utilisation du Journal d'événements :

1. Pour ouvrir l'Observateur d'événements, cliquez sur le bouton **Démarrer**, sur **Panneau de configuration**, sur **Système et sécurité**, sur **Outils d'administration**, puis double-cliquez sur **Observateur d'événements**. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, fournissez le mot de passe ou la confirmation.
2. Cliquez sur un journal des événements dans le volet de gauche.
3. Double-cliquez sur un événement pour en afficher les informations.

3-Création et suppression des journaux des événements personnalisés

La classe **EventLog** vous permet de créer un journal des événements personnalisé sur un ordinateur local ou distant. Ce type de journal est utile si vous voulez archiver vos entrées d'une manière plus précise que celle qui est disponible lorsque vos composants ajoutent des entrées dans le journal d'applications

par défaut. Supposons qu'un composant **OrderEntry** entre des informations dans un journal des événements. Vous voulez effectuer une copie de sauvegarde des entrées et les conserver plus longtemps que les entrées du journal d'applications. Pour éviter qu'une fois inscrit, le composant ajoute des entrées dans le journal d'applications, vous pouvez créer un journal des événements personnalisé que vous nommez **OrdersLog**, puis inscrire le composant de manière à ce que celui-ci consigne les entrées dans ce journal. Ce faisant, toutes les informations sont stockées au même endroit et elles ne sont pas affectées par la suppression des entrées du journal d'applications.

La méthode **CreateEventSource** peut être utilisée, de manière indirecte, pour créer un journal des événements personnalisé. Cette méthode crée une nouvelle source et vous permet de spécifier dans quel journal des événements les entrées doivent être ajoutées. Si le journal des événements spécifié n'existe pas, le système crée automatiquement un journal des événements personnalisé et inscrit votre composant en tant que source de ce journal.

Remarque :

La suppression d'un journal des événements personnalisé se fait de la même manière que n'importe quel autre journal, à l'aide de la méthode Delete. Pour plus d'informations,
consultez Suppression d'un journal des événements.

4- Gestion des journaux :

Pour effectuer une action sur un journal il faut faire un clic-droit sur le journal concerné.

Liste des actions que vous pouvez effectuer sur un journal **:**

- Ouvrir un fichier journal, permet de lire et d'afficher le contenu d'un journal ;

- Enregistrer le fichier journal sous, permet de sauvegarder le fichier journal ;
- Nouvel affichage du journal, permet de dupliquer à l'identique un journal ;
- Effacer tous les événements, permet de vider complètement un journal Affichage.

    - Ajouter / Supprimer des colonnes ;
    - Tous les enregistrements, permet d'afficher la totalité des événements d'un journal ;
    - Filtrer, permet la sélection et/ou l'omission pour l'affichage de divers événements par leur type, source, catégories, ID, Utilisateur, tranche de dates & heures ... ;

    - Plus récents / plus anciens d'abord, permet de modifier l'ordre de tri pour l'affichage du journal (par ordre croissant/décroissant de date et heure) ;
    - Rechercher, permet de localiser un événement précis d'après certains critères ;
    - Personnaliser, permet de définir l'interface de l'observateur d'événements.

- Renommer, permet de modifier le nom du journal ;
- Actualiser, rafraichis et affiche la sélection en cours des événements ;
- Exporter la liste, permet de sauvegarder le journal dans un fichier texte ou CSV (Séparateur : virgule ou tabulation) ;
- Propriétés, permet d'afficher toutes les propriétés du journal et effectuer certaines manipulations **:**

    - Modifier sa taille ;
    - Définir le type d'épuration des événements à effectuer quand le fichier a atteint sa taille maximale ;
    - Réinitialiser les paramètres par défaut ;
    - Effacer le journal ;
    - Filtrer les événements du journal.

RAPPORT D'INTERVENTION

DESIGNATION MACHINE **NOM :** **MARQUE :**

TYPE : **ZONE :** **N° :** **BATIMENT :**

NOM DE L'INTERVENANT :…….CLASSE :……

DATE	**TEMPS ALLOUE 4 H**	**TEMPS PASSE**
……		**……..**

DEFAUTS CONSTATES OU TRAVAIL DEMANDE :……..……

……

……

……

CAUSES POSSIBLES	OPERATIONS
- ……	❒ SECURITE ❒ PNEU
- ……	❒ HYDRAU ❒ ELEC
- ……	❒ MECANIQUE ❒ PREVENTIF
- ……	❒ CORRECTIF

REPARATION OU INTERVENTION EFFECTUEE :

……

……

……

OUTILLAGE UTILISE :

……

……

CONCLUSION-SUGGESTIONS

……

……

http://igm.univ-mlv.fr/~duris/NTREZO/20032004/Charpentier-Montigny-Rousseau-VirusAntivirus.pd